Electronic Version

Stylesheet Version v1.1.1

Description

[DataVault X4 Multi-Network Secure Computer]

BACKGROUND OF INVENTION

[0001] This invention relates to a multilevel network secure computer system built within a custom secure case which is comprised of two or more hardware domains that are active concurrently. This system can switch between the classified and unclassified domains instantly and control user access to the computer itself and the secure network without powering down one domain and then re-booting and powering up to the second or third domain. Subsequently this results in no data loss and no switching delays. The final result is instant viewing of classified or unclassified data in one computer case without any chance of data being compromised. This is achieved using hardware-based technology and without any shared devices within the system. The case and the power supply are the only shared devices.

SUMMARY OF INVENTION

[0002] Prior design of multilevel computer systems include the use of complicated mechanical switching mechanisms (Patent 6,009,518) or the addition of complex circuitry with relays and microprocessors controlled via automatic teller machine (ATM) styled keypads requiring a personal identification number (PIN) for switching from one network domain to the other by powering down one domain and powering up to another domain. (Patents 6,389,542, / 6,351,810) These systems result in total loss of data between one domain to the other during switchover which includes operating system shutdown and re-booting along with substantial switching time delays. Most of such computer systems share the same central processing units (CPU), random access memory (RAM), universal serial bus (USB) controllers, video memory, floppy drives, and compact disk read only memory (CD-ROM) drives. They also use commonly available Smart Card® readers/writer technology for additional user access control.

[0003] The objective of this invention is to provide a custom-built secure multilevel computer system to provide data security from within and prevent inside unauthorized user access as well as outside unauthorized user access via the

Internet or a network. This invention was requested by the Department of Defense, the Pentagon and other government agencies to be used in critical operating environments for secured and unsecured networks that need to be viewed without delays. These environments require processing of unclassified and classified data instantly and without compromising data security between domains and without powering down and re-booting between domains which results to data loss upon switching between domains contained in the same computer.

[0004] The benefits of this technology other than data security include; instant domain switching, reduced footprint, reduced power consumption, reduced heat output, reduced EMF emissions, reduced maintenance and acquisition costs, and reduced operating system costs.

Brief Description of Drawings

[0005] Figure 1 is a block diagram of the DataVault X4 Multi-Network Computer.

[0006] Figure 2 is the rear view of the DataVault X4 Multi-Network Computer.

[0007] Figure 3 is the front view of the DataVault X4 Multi-Network Computer.

Detailed Description

[0008] By implementing a physical hardware access control of the specially constructed computer case itself via a hardware lock/key cover for the front of the computer case as well as the back, ensures a solid access control to the physical hardware itself before the computer can be turned on via an electro-mechanical key lock which is similar to the ignition key of a vehicle.

[0009] Each hardware domain within the specially constructed cast iron computer case has its own CPU, memory, motherboard, network card, video card, sound card, hard drive, floppy drive, parallel and serial ports, USB, CD-ROM drive and separate color-coded reset buttons, (red and green) on the front side of the computer case. The red button indicates the secured domain hardware reset and the green indicates the unsecured domain hardware reset. Each hardware domain can be re-booted and restarted independently without affecting the other domain, during software installations. The Smart Card® reader/writer is connected only on the secured hardware domain which provides access to authorized users only. A third optional hardware domain can be controlled through the same access control method using the Smart Card® reader/writer.

[0010] Upon powering-on the computer using the physical key in

the lock which is in the front of the computer case, both hardware domains activate and access to the unsecured domain is available by default. The unsecured domain is defined by its own memory device or hard drive for storing data which by definition is a domain level with unrestricted access. The first domain level with unrestricted access may further have a modem device for telecommunication for internet access as well as a network card for unsecured network access. The unsecured domain also has its own independent read-only memory device such as CD-ROM and a floppy disk drive labeled with a green dot for easy identification.

[0011] By pressing the red button on the electronic KVM (keyboard/video/mouse) switch, access to the second domain level is restricted by the Smart Card® reader/writer. The authorized user must then insert his own personal ID card into the Smart Card® reader/writer for access and user identification and authentication by entering his PIN (personal identification number or password). Once a PIN number is entered, the authorized user can proceed and access the secured domain or classified network. At any time the authorized user wishes to switch to the unsecured domain network, he or she can do so by pressing

the unsecured button on the KVM switch and instantly access the internet or unsecured network without having to shut down the secured domain and re-boot the unsecured domain. The authorized user can switch back to the secure domain by pressing the secured button on the KVM switch within less than a second without re-powering or re-booting domains and without a loss of data on either domains.

[0012] The secured domain is also defined by its own memory device and a removable hard drive case with a lock key, for storing data, which by definition is a domain level with restricted access. The secured domain also has its own independent read-only memory device such as compact disk CD-ROM and a floppy disk labeled with a red dot for easy identification. When the secured domain authorized user completes his or her assignment, they can then perform normal system shutdown and remove the secured domain's hard drive without affecting the operation of the unsecured domain.

[0013] In order to ensure that data may not bleed-over from the unsecured domain and network to the secured domain and network within the case, the motherboards and network devices were placed with three inches apart and

were separated with a special microwave aluminum shield. This shield assures the integrity of data access control, data storage, and data communications for both the secure and unsecured sides of the computer will remain in tact emphasizing that top level security will be maintained for classified network activities.

[0014] The physical back cover key/lock prevents unauthorized users from manipulating network cables between the secured and unsecured domains as well as preventing removal of other devices such as video/keyboard/mouse cables.

[0015] The DataVault X4 offers a solid hardware based security solution that securely processes and stores unclassified and classified data without requiring two separate computers to achieve this effect. The Data Vault X4 incorporates a non-software dependent electro-mechanical key-lock that requires a high level security key to activate it, and this key cannot be removed while in operation nor can it be duplicated. The removable classified hard drive on the secured domain requires a key for removal since classified hard drives must be placed in a safe when not in use. The second layer of security for the classified domain is implemented through the built-in dedicated Smart

Card® reader/writer that provides access control and user identification and authentication. The DataVault X4 has the security functionality of up to three separate computers in a single cost-effective workstation. A single DataVault X4 requires only one software license, monitor, keyboard and mouse and dramatically reduces heat output, power consumption and space requirements by at least one half, along with significantly reducing maintenance, life-cycle and repair costs of the multiple computers that it could replace. DATAVAULT X4 COMPONENTS (FIG. 1)The DataVault X4 is built in a heavy-duty cast iron computer case (1) especially designed to accommodate 14 expansion slots instead of the traditional 6 or 8. The case has a low EMF radiation output level and a 350 watt power supply, (3) one electronic on/off switch (2) and one hardware access control electronic/mechanical keyed switch (4) for identification/authentication. Within the case are two completely isolated and independent domains, one unsecured (Designated "U") for general use and one secure (Designated "S") each with an isolated reset button (10 & 13) respectively. Both domains operate and are active concurrently. Each domain contains two isolated memory banks (5 & 9), two isolated CPU (11 & 12), two

isolated hard drives (18 & 19 where the secure hard drive is removable), two isolated network cards (NIC), (16 & 17), two isolated video cards (24 & 25), two isolated 3.5 inch Floppy/DVD CD-ROM combo drives (20 & 21), and two isolated keyboard/mouse controllers. (26 & 27) Each of these pairs of components are on the respective secure and unsecured sides of the computer. The unsecured side of the computer also has an optional modem feature (25) and both sides of the computer have optional sound card features. (22 & 23)The secure side of the computer incorporates a Smart Card® reader/writer (15) for an additional layer of security for user access and identification/authentication. An EMF shield (7) separates the unsecured side from the secure side of the computer so data bleed-over does not otherwise compromise data integrity and security. One external digital electronic switch (28) operates the swapping of a single keyboard (31), single video monitor (32), and single mouse (33) from the unsecured to the secure domain. Each interchange from one domain to the other takes place in approximately one second using buttons S1 and S2 (29 & 30) respectively. No system-wide reset or shutdown is necessary when switching domains. Both domains remain active with no data loss tak-

ing place on either domain when switching to the other respective domain and back again on demand by the authorized user and without delay for rebooting.

[0016] EXTERNAL REAR VIEW DATAVAULT X4 (FIG. 2)The DataVault X4 has 14 slots across the rear of the case. Slots 34 through 39 reside on the secure side of the computer. From left to right they range from a USB card, optional sound card, a combination COM/LPT port card, video card and two open slots respectively. Separating the secure side from the unsecured side of the computer is an EMF radiation shield that physically separates the two domains and motherboards respectively. (40) Slots 41 through 47 reside on the unsecured side of the computer. From left to right they range from a USB card, optional sound card, a combination COM/LPT port card, video card, optional modem and two open slots respectively.

[0017] A cooling fan (48) and two AC connections are on the left rear side of the case. One male AC connection (49) for connecting the computer power supply to 110 volt electrical current and one female AC connection (50) for supplying 110 volt current to a monitor. A locking (53) tamperproof rear cover (51) with apertures (54) for cables to exit respective opposite directions of the secure and unse-

cured sides of the computer insure cables can not be switched and therefore maintain data integrity for the two separate networks.

[0018] EXTERNAL FRONT VIEW DATAVAULT X4 (FIG. 3)The DataVault X4 is first accessed by inserting a physical key in a mechanical keyed lock (Fig. 65) on the front cover (64) mounted on a tamper-proof metal hinge. (66) An electro- mechanical lock on the front of the computer requires a physical high-level key to first turn-on (55) the computer and boots both domains of the computer up simultaneously. The unsecured side is accessible immediately upon booting by default and so is the domain and network. To access the secure side of the computer the red button is pressed on the KVM (keyboard/video/mouse) electronic switch (59) which prompts the authorized user to insert a Smart Card® into the Smart Card® reader/writer (56) and a PIN number is requested. Authorization is granted upon entering the correct PIN code. To move back to the unsecured domain, the green button (62) on the KVM electronic switch is pushed and immediate switching occurs to the unsecured domain without reset or re-booting and without data loss.

[0019] A removable secure hard drive (57) with a built-in key/

lock allows removal for safe storage when the computer is not in use, which is located above the two secure and un-secured 3.5 DVD-CD ROM combo drives respectively. (60 63) A cooling fan with replaceable air filters (58) adds cooling power to the power supply needed for running the dual or triple motherboards and an LED panel (61) keeps the user abreast of vital information while at operation of the DataVault X4.